

## 4000 SECTION - PREVENTION

- 4100 INTRODUCTION
- 4200 MARITIME SECURITY MARSEC LEVEL PLANNING
  - 4210 Link to Homeland Security Advisory System
  - 4220 Procedures when vessel & facility are at different MARSEC
  - 4230 Procedures for requesting equivalencies to MARSEC Directives
- 4300 MARSEC LEVEL 1
  - 4310 Standard Security Procedures for MARSEC Level 1
  - 4320 Physical Security Measures
  - 4330 Operational Security (OPSEC) Measures
  - 4340 Roles, Resources, Authorities, and Responsibilities
  - 4350 Sea Port of Embarkation Operational Plan
- 4400 MARSEC LEVEL 2
  - 4410 Standard Security Procedures for MARSEC Level 2
  - 4420 Physical Security Measures
  - 4430 Operational Security Measures
  - 4440 Roles, Resources, Authorities, and Responsibilities
  - 4450 Sea Port of Embarkation Operational Plan
- 4500 MARSEC LEVEL 3
  - 4510 Standard Security procedures for MARSEC Level 3
  - 4520 Physical Security Measures
  - 4530 Operational Security Measures
  - 4540 Roles, Resources, Authorities, and Responsibilities
  - 4550 Sea Port of Embarkation Operational Plan
- 4600 PUBLIC ACCESS FACILITY
  - 4610 Designation of Public Access Facilities
  - 4620 Withdrawal of Designation
  - 4630 Security Procedures for Public Access Facilities
- 4700 MARITIME WORKER CREDENTIALS

### 4100 (U) Introduction

MARSEC Levels were established to allow the Coast Guard to easily and clearly communicate the security measures required in response to an HSAS Threat Condition. MARSEC Levels permit FMSCs, in consultation with the Port Security Committee, to plan and pre-designate appropriate preventative and protective postures for each MARSEC Level. The three MARSEC Levels align with the five color-coded HSAS Threat Conditions. Because of the unique nature of the maritime industry, MARSEC Level 1 applies when HSAS Threat Conditions Green, Blue, and Yellow are set. MARSEC Level 2 corresponds to HSAS Threat Condition Orange, while MARSEC Level 3 corresponds to HSAS Threat Condition Red.

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-1
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

## 4200 (U) Maritime Security (MARSEC) Level Planning

This section is organized as follows:

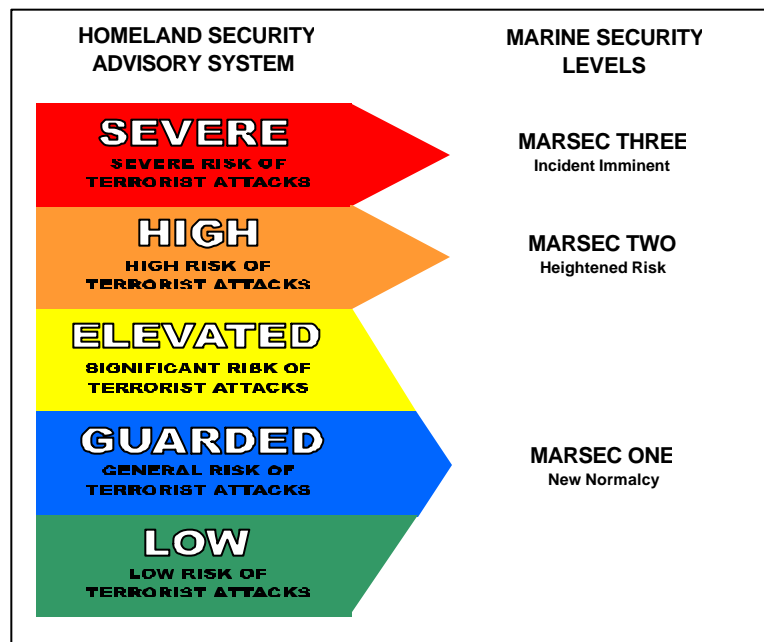
- 4210 [Link to Homeland Security Advisory System](#)
- 4220 [Procedures when a Vessel and Facility are at Different](#)
- 4230 [Procedures for Requesting Equivalencies to MARSEC Directives](#)

### 4210 (U) Link to Homeland Security Advisory System

Given that the Secretary of the Department of Homeland Security manages HSAS Threat Conditions as a national system, only the Commandant of the Coast Guard can set MARSEC Levels, such MARSEC changes will occur when the threat that prompted a change in the HSAS Threat Condition imperils the MTS.

There may be instances where DHS raises the HSAS Threat Condition based on threats unrelated to the MTS, the threat becomes more defined and it is clear that the MTS is not a target. In these instances, the Commandant may set MARSEC Levels below the equivalent HSAS Threat Condition. Furthermore, it may be appropriate for the Commandant to raise the MARSEC Level at only specific ports in response to the elevated HSAS Threat Condition instead of requiring all ports nationwide or on a particular coast to elevate their protective measures. Examples include ports where military load-outs occur or those considered strategically important.

FMSCs may temporarily raise the MARSEC Level in their respective AOR or for a segment of the maritime industry within that area only when there is a serious threat to the MTS requiring immediate action to prevent a TSI and timely consultation with the Commandant is not feasible. The heightened MARSEC Level will continue only as long as necessary to address the serious threat which prompted the FMSC to set that Level. An example would be a situation where a FMSC receives information from the local police that a bomb has been located at an LNG facility while a Liquefied Natural Gas (LNG) ship is inbound to the facility. It is anticipated that COTPs would raise the MARSEC Level only in the most rare of circumstances.



VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-2
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

## 4220 (U) Procedures when Vessel and Facility are Different MARSEC Levels

There may be circumstances (i.e. directed by their flag state or at the discretion of the vessel owner) where a vessel is operating at a higher MARSEC Level, as defined by the ISPS Code, than the port that the vessel is calling on. In such cases, the port and its facilities may remain at the existing MARSEC Level. However, if the port or facility is at higher MARSEC Level per Commandant or FMSC direction than the arriving vessel, the foreign flagged vessel must attain the corresponding MARSEC Level. The assumption is made that U.S. flagged vessels will already be at a corresponding MARSEC level with the receiving facility but the ship's agent is still responsible for prior notification of the facility's and vessel's MARSEC Levels.

The responsibility to notify adjacent facilities within 500 meters of the receiving facility of the higher MARSEC Level of the arriving ship remains with the receiving facility. The arriving foreign flagged vessel that is at a higher MARSEC Level must submit a plan along with their Notice of Arrival ninety-six hours in advance to and the receiving facility via the ship's agent that describes how it expects the facility to help accommodate the higher level of security.

Since the regulations require the facility to determine the MARSEC Level of those vessels arriving at its facility, the facility must work with both the ship's agent and FMSC to assure that all notifications are made as to the applicable and required MARSEC Levels.

## 4230 (U) Procedures for requesting equivalencies to MARSEC Directives

MARSEC Directives will set mandatory measures that all defined entities must meet in a specified time period. These entities will also be required to confirm, to the local COTP, receipt of the MARSEC Directive, as well as specify the method by which the mandatory measures have been (or will be) met. If a MARSEC Directive recipient is unable to implement the measures mandated in the MARSEC Directive, the recipient may propose temporary equivalent security measures to the local COTP. However, the recipient will only be able to propose such equivalencies for the shortest period of time possible never to exceed the length of the MARSEC Directive, and it will be required to implement any portion of MARSEC Directive where the COTP does not approve a proposed equivalency. These facilities or vessels may receive verbal permission from COTP for a temporary waiver, to be documented by the Integrated Command Center, to be followed up with documentation submitted to the COTP within a period not to exceed six hours. See section 3400.

Time allotted to comply to MARSEC Directive	Time required for submission of Temporary Security Measures	Time allotted for complete implementation of MARSEC Directive
12 hours	6 hours	Not to exceed length of Directive

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-3
--------------	-------------	----------------------------	-----------------------	--------------	-------------------	------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sections 104.130, 105.130, and 106.125 state that vessel or facility owners or operators requesting Alternate Security Program waivers for any requirement of part 104, 105, or 106 must include justification for why the specific requirement(s) are unnecessary for that particular owner's or operator's vessel or facility or its operating conditions. A request for a waiver must be submitted in writing with justification to the Commandant (G-MP) at 2100 Second St. SW., Washington, DC 20593.

## 4300 (U) MARSEC Level 1

This section is organized as follows:

- 4310 Standard Security Procedures for MARSEC Level ONE
- 4320 Physical Security Measures
- 4330 Operational Security (OPSEC) Measures
- 4340 Roles, Resources, Authorities, and Responsibilities
- 4350 Security Measures for SPOE Operations

## 4310 (SSI) Standard Security Procedures for MARSEC Level ONE

[RESERVED]

## 4320 (SSI) Physical Security Measures

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(1)	UNCLAS	FBI JTTF / FDLE RDSTF / MJTF J-2	Create a declassified single combined Northeast and Eastern Central Florida Maritime Threat Assessment at the SSI INFOSEC level and circulate to all MJTF members and all port entities required to write or update MTSA vessel or facility security plans.
(2)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(3)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(4)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(5)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(6)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-4
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(7)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(8)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(9)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(10)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(11)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(12)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(13)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(14)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-5
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(15)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(16)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(17)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(18)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(19)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(20)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(21)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(22)	UNCLAS	CDC Quarantine Station, JMTF Harbor Safety Committee, USCG Captain of the Port	Designate three offshore quarantine anchorages for Jacksonville / Fernandina as holdings areas for: (1) suspected biological vectors - closest to shore; (2) suspected chemical vectors - intermediate distance offshore; and (3) suspected radiological vectors - as near the 12 NM limit as possible.
(23)	UNCLAS	CDC Quarantine station and USCG Captain of the Port	Designate three offshore quarantine anchorages for Port Canaveral as holdings areas for: (1) suspected biological vectors - closest to shore; (2) suspected chemical vectors - intermediate distance offshore; and (3) suspected radiological vectors - as near the 12 NM limit as possible.

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-6
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(24)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(25)	UNCLAS	USCG	Establish 25 meter permanent no-entry security zones around all international cruiseship terminals, marine events with more than 1000 persons estimated to attend, and passenger staging areas with more than 1000 persons contained in a small shoreline area.
(26)	UNCLAS	Facility Operators and Marine/Shoreline Event Organizers	Establish periodic monitoring of the security zones established by measure (25); assure monitoring is low-light capable and establish hot-line procedures for emergency notification of an intrusion (from water or shore) to 911 and the Coast Guard Integrated Command Center at (904) 247-7318.
(27)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(28)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(29)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(30)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(31)	UNCLAS	ALL	Conduct annual Area Maritime Security Exercises, audits, and drills. Conduct required facility and vessel security exercises, audits, and drills under 33 CFR part 104 and 105. Periodically review the Area Plan and emergency response plans for familiarization and currency (at least once per year).
(32)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-7
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(33)	UNCLAS	USCG	Halt the operation of all facilities subject to 33 CFR part 105 that do not have approved Facility Security Plans not later than 01 July 2004. Inspect facilities with approved plans for security purposes and spot - check/test security at these facilities at least once per year.
(34)	UNCLAS	USCG	Halt the operation of all vessels subject to 33 CFR part 104 that do not have approved Vessel Security Plans not later than 01 July 2004. Inspect vessels with approved plans for security purposes and spot - check/test security at these vessels at least once per year.
(35)	UNCLAS	USCG	Ban foreign vessels subject to the International Ship and Port Facility Security Code (ISPS) that do not have approve vessel security plans from U.S. waters by 01 July 2004. Inspect vessels with ISPS security plans at least once per year to verify their security plans are in place and security measures are executed in accordance with it.
(36)	UNCLAS	USCG	Conduct second-tier reviews of any vessel in violation of the Advanced Notice of Arrival regulations. Issue COTP orders to hold any vessel approaching from entering the Northeast and Eastern Central Florida ports until such time as the second-tier review of the vessel is complete. Lift the COTP order only when the vessel has screened low-risk.
(37)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(38)	UNCLAS	MJTF J-2	Visit major marinas monthly to review activities for suspicious behavior, establish rapport, and monitor for signs of terrorist, organized crime, or illegal protest activity, logistics, or reconnaissance.
(39)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(40)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-8
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.



<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(41)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(42)	UNCLAS	All Government	Fascilitate training for field-level government and private security personnel on recognizing: (1) chemical and radiological augmented IEDs; (2) routine IEDs; (3) biological vectors such as weaponized Anthrax; (4) symptoms and signs of virulent disease outbreaks (whether naturally occurring or as terrorist vectors).
(43)	UNCLAS	All	Treat all unauthorized persons / unidentified intruders as hostiles and enact CBRNE response measures (particular focus on planted CBRNE devices) until threat has been deemed non-credible (fail-safe posture).
(44)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(45)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(46)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(47)	UNCLAS	All	Maintain readiness to execute MARSEC TWO security measures in this plan and in approved facility security plans within twelve (12) hours. Review MARSEC TWO security measures in this plan and approved VSPs/FSPs at least once per quarter.

## 4330 (SSI) Operational Security (OPSEC) Measures

Operational Security is defined as a systematic and analytical process by which Government agencies, commercial entities, and private citizens can deny potential adversaries information about our capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.

The information about our intentions, capabilities, or activities is known as “critical information.” Since the compromise of this critical information may allow a terrorist to gain a significant advantage, its protection involves all personnel—active, reserve, auxiliary, civilians and contractors. A concerted effort must be taken to ensure everyone is aware that the threat is real and active in all aspects of our missions.

Operational Security Measures mitigate or control vulnerabilities, threats, and usefulness of information that our adversaries may develop. These measures can include procedural changes,

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-9
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	--------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

suppression of indicators to deny critical information, deception, preception management, intelligence countermeasures, traditional (physical) security measures, or any other action that is likely to thwart our adversary's purposes. The Port Security Committee has recommended the following OPSEC Measures for MARSEC ONE:

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(O-1)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-2)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-3)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-4)	UNCLAS	All	Minimize to the extent possible budgetary limitations related to security measures, systems, and forces are made public.
(O-5)	UNCLAS	All	Protect the security training status and records of personnel – make it difficult to learn who has completed what training and for what purpose they were trained.
(O-6)	UNCLAS	All	Avoid descriptive or easily associated project names and exercise names, acronyms, and nicknames in conducting security business.
(O-7)	UNCLAS	All	Periodically conduct surveillance of your own property and/or operation and identify signals/patterns/indicators that alert observers when you are about to conduct specific critical operations (e.g., pier lights always energized ½ hour before vessels arrive), and re-design so that these indicators are used for a variety of operations and periodically employed when no operation is on-going, thereby eliminating their value as true indicators for adversary surveillance.
(O-8)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-9)	UNCLAS	All	Review web-sites and public calendars that would indicate locations/schedules/activities of executives and critical personnel and remove these sites.
(O-10)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

## 4340 (SSI) Roles, Resources, Authorities, and Responsibilities

[RESERVED]

## 4350 (SSI) Security Measures for SPOE Operations

[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-10
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

## 4400 (U) MARSEC Level 2

This section is organized as follows:

- 4410 Standard Security Procedures for MARSEC Level TWO
- 4420 Physical Security Measures
- 4430 Operational Security Measures
- 4440 Roles, Resources, Responsibilities
- 4450 Security Measures for SPOE Operations

## 4410 (SSI) Standard Security Procedures for MARSEC Level TWO

[RESERVED]

## 4420 (SSI) Physical Security Measures

Measure	Info Security	Responsible Entity	Description
(48)	UNCLAS	All	Continue all MARSEC ONE Security Measures except measures (31), (32), (38), and (42).
(49)	UNCLAS	All vessels and facilities with required security plans, all government installations	<b>Conduct an OPERATIONAL PAUSE</b> while all spaces and operations ashore and afloat are reviewed. No vessels are to depart the dock or make entry into the port. Re-start operations after all-clear is confirmed by FSO/VSO. Report the all-clear as soon as possible and no later than two hours after notification to the USCG Integrated Command Center, <b>3440.2</b> . Report suspicious activity or security breaches to 911 and the National Response Center at (800) 422-8802. For entities with approved facility or vessel security plans, begin implementing MARSEC TWO security measures after the operational pause is complete and confirm attainment of MARSEC TWO within twelve hours. Report inability (shortfalls) to attain elements of MARSEC TWO security measures immediately to the USCG Integrated Command Center. Repeat review/search procedures every 12 hours while MARSEC TWO is maintained, including report of "all clear" to the Integrated Command Center, <b>3440.2</b> .
(50)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-11
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(51)	UNCLAS	USCG Captain of the Port	Issue/activate Security Zone regulations and Broadcast Notices to Mariners requiring all pilots and operators of vessels over 50 meters in length (tug operators for barges over 50 meters in length) intending to transit the following areas to contact and clear with the Coast Guard/MJTF vessel serving as Sentinel/Gate-keeper offshore before making inbound or outbound transits: (1) St. Marys River and the ICW from Kings Bay to the ocean and three miles around the mouth to the St. Marys River; (2) St. Johns River from Dames Point Cruise Terminal to the ocean and three miles around the mouth to the St. Johns River; (3) Port Canaveral and three miles around the entry to Port Canaveral; and (4) all federal anchorages as defined in 33 CFR 110.183.
(52)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(53)	UNCLAS	USCG Captain of the Port	Upon MARSEC TWO set, issue a general Captain of the Port order prohibiting the entry and departure of vessels except law enforcement and emergency response as part of the Operational Pause. Once an all-clear has been reported, grant permission for the vessel to resume operations, and lift the general Captain of the Port Order only when the large majority of vessels and facilities requiring security plans have reported all-clear.
(54)	UNCLAS	Owners of properties located within 100 meters of a bridge over the Intercoastals Waterway, St. Johns River, Banana River, or Indian River	Upon MARSEC TWO set, review all operations on your property or by tenants on your property as part of the Operational Pause and conduct a search of your property for unauthorized vehicles and/or placed packages/bins/containers which could be Improvised Explosive Devices (IEDs) endangering the bridge and/or its supports. Report suspicious vehicles and packages to the police at 911 and the Coast Guard Integrated Command Center (904) 247-7318. Report the all-clear to the Coast Guard Integrated Command Center (see paragraph <b>3440.2</b> ) as soon as possible and in no case more than two hours after MARSEC TWO set. Conduct a similar search/review at least once every 48 hours and report the all-clear to the Coast Guard Integrated Command Center.
(55)	UNCLAS	Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons	Upon MARSEC TWO set, review all operations on your property or by tenants on your property as part of the Operational Pause and conduct a search of your property for unauthorized vehicles and/or placed packages/bins/containers which could be Improvised Explosive Devices (IEDs) endangering the areas where people congregate. Report suspicious vehicles and packages to the police at 911 and the Coast Guard Integrated Command Center at (904) 247-7318. Report the all-clear to the Coast Guard Integrated Command Center (see paragraph <b>3440.2</b> ) as soon as possible and in no case more than two hours after MARSEC TWO set. Conduct a similar search/review at least once every 48 hours and report the all-clear to the Coast Guard Integrated Command Center.

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-12
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(56)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(57)	UNCLAS	Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons	Limit the total number of people attending your events / congregating and/or disperse people in your buildings/attending events/congregating such that the density of persons limits the number of people to 1000 within a 25 meter radius, thereby limiting the consequences of an Improvised Explosive Device attack by limiting the number of people inside IED stand-off distance. Review and remove as much as possible anything that is likely to serve as secondary debris for an IED detonated anywhere within your event/congregation area/building. To the extent possible, re-locate congregation areas/high-density areas away from exterior walls and windows thereby reducing vulnerability to IEDs detonated in proximity to outsides of building and reducing flying debris impacts.
(58)	UNCLAS	Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons	Review and limit as much as possible the number of vehicle access points to your event, building, or passenger staging area. Limit vehicle approaches to 10 meters of congregation/inhabited areas. Because the energy of an approaching vehicle (laden or unladen with explosives) increases with the square of the speed of the vehicle, increase the stand-off distances to congregation areas in the direct path of high-speed approaches (straight-on streets, etc.). Wherever possible move congregation areas, etc., into areas at a tangent to high-speed approaches. Minimize vehicle speeds in areas under your control. Conduct IED sweeps on all vessels coming alongside prior to approach, particularly on passenger vessels, while passengers are present (bunker when passengers are not present).
(59)	UNCLAS	Shoreline Buildings, Marine/Shoreline Event Organizers, and Passenger Staging Area Managers with more than 1000 persons	Review likely vantage points for terrorist, organized crime, and illegal protest surveillance of your buildings, congregation areas, and vehicle or pedestrian access points, even when those vantage points are outside your area of control. To the extent possible, place obstructions and screens to reduce visibility of your operations/event/areas from those likely vantage points.
(60)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(61)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-13
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(62)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(63)	UNCLAS	FL National Guard Civil Support Team	Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
(64)	UNCLAS	Florida Department of Health	Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
(65)	UNCLAS	USN Commander, Navy Region Southeast	Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
(66)	UNCLAS	Commanding General, Patrick Air Force Base and Director Kennedy Space Center	Activate and deploy personnel to the MJTF Unified Command Incident Command Post.
(67)	UNCLAS	MJTF	Initiate and maintain close liaison with CDC Quarantine Station in Miami.
(68)	UNCLAS	MJTF	Deploy liaison officer assistants to the Brevard, Duval, and Nassau County Emergency Operations Centers (MACCs within the National Response Plan framework) for interagency coordination outside the Marine division. All federal, state, and local governmental marine entities will be integrated into MJTF Unified Command and represented as assigned within the MTJF ICS.
(69)	UNCLAS	MTJF	Deploy liaison officer assistants to the FBI Emergency Operations Center and FDLE Emergency Operations Center if activated.
(70)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(71)	UNCLAS	USCG Captain of the Port	Maintain and continuously track through the MTJF-ICC all shortfalls reported by facilities and vessels with approved security plans. Evaluate shortfalls and where shortfalls create a manifestly unsafe condition in view of MARSEC TWO Threat Information, issue Captain of the Port Orders halting operations and/or closing the security shortfall. Where MJTF resources/efforts are required to close the gap, assign same as a priority to the MJTF Unified Command. Update and include gap-closing measures in the Common Operational Picture (COP) and coordinate continued MJTF reconnaissance on shortfalls where necessary to evaluate required gap-closing security measures.

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-14
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(72)	UNCLAS	USCG Captain of the Port	Issue/activate RNA regulations and Broadcast Notices to Mariners forbidding mooring to or loitering in the vicinity of all bridges over the ICW, St. Marys River, St. Johns River, Banana River, Indian River, Barge Canal (Canaveral), and Hanover Canal.
(73)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(74)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(75)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(76)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(77)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(78)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(79)	UNCLAS	MJTF, Facility Operators and Marine/Shoreline Event Organizers	Increase monitoring of security zones around terminals and high-density marine/shoreline events defined in MARSEC ONE Security Measure (25) to continuous low-light capable monitoring plus periodic patrols by security personnel (from ashore acceptable) on a randomly-timed, randomly-rotating frequency of patrol basis.
(80)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-15
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(81)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(82)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(83)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(84)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(85)	UNCLAS	USCG Captain of the Port	Within 24 hours of MARSEC TWO set, hold open-session Port Security Committee meetings in Jacksonville/Fernandina and Port Canaveral to refresh all personnel on this plan, MARSEC TWO security measures, recognition of CBRNE vectors and devices, and the specific threat information.
(86)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(87)	UNCLAS	USCG and FDEP	Within 24 hours of MARSEC TWO set, alert all pollution response contractors to attain heightened deployment readiness. Review Area Contingency Plan, Hazardous Materials Annex, and County Disaster Response Plans, <u>reference ACP call out list.</u>
(88)	UNCLAS	USCG, FWCC, and FDLE	Deploy auxiliary support officers throughout boating community at marinas stores, dives shops, etc., to assure maximum awareness of MARSEC TWO security zones, restrictions, and issues. Maintain continuous effort throughout MARSEC TWO.
(89)	UNCLAS	All	Maintain readiness to execute MARSEC THREE security measures in this plan and in approved facility security plans within twelve (12) hours. Review MARSEC THREE security measures in this plan and approved VSPs/FSPs within six hours of MARSEC TWO set.

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-16
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.



## 4430 (SSI) Operational Security Measures

Operational Security is defined as a systematic and analytical process by which government agencies, commercial entities, and private citizens can deny potential adversaries information about our capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.

The information about our intentions, capabilities, or activities is known as “critical information.” Since the compromise of this critical information may allow a terrorist to gain a significant advantage, its protection involves all personnel—active, reserve, auxiliary, civilians and contractors. A concerted effort must be taken to ensure everyone is aware that the threat is real and active in all aspects of our missions.

Operational Security Measures mitigate or control vulnerabilities, threats, and usefulness of information that our adversaries may develop. These measures can include procedural changes, suppression of indicators to deny critical information, deception, preception management, intelligence countermeasures, traditional (physical) security measures, or any other action that is likely to thwart our adversary’s purposes. The Port Security Committee has recommended the following OPSEC Measures for MARSEC TWO:

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(O-11)	UNCLAS	All	Continue all MARSEC ONE and OPSEC Measures except (O-1), (O-3), (O-8), (O-9), and (O-10).
(O-12)	UNCLAS	All	Schedule operations and activities simultaneously so they mask each other and confuse observers as to what is happening and how the operations are related (if at all).
(O-13)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-14)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-15)	UNCLAS	All	Disrupt anyone who might be monitoring/surveilling your operations by occasionally rotating your communications procedures (from radio to cell phone to land-line) etc.
(O-16)	UNCLAS	MJTF	Within four hours of MARSEC TWO set, begin monitoring of OPSEC measures within the port and on vessels. Assure vessels, facilities, and other marine areas are using these OPSEC measures and those defined within their own security plans.

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-17
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(O-17)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-18)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-19)	UNCLAS	All	Gradually change your activity levels to meet MARSEC TWO requirements so the change is less apparent; gradually slow your activity levels after “operational pause” that the observers will not readily understand when the operational pause has ceased.
(O-20)	UNCLAS	All commercial entities	Without disrupting operations, time activities to occur during periods of least security vulnerability,e.g. avoid scheduling delivery of stores during passenger embarkation.
(O-21)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-22)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-23)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-24)	UNCLAS	All	To the extent possible, change the critical personnel reporting times and operational cycles in order to maximize adversary confusion. Vary the times and routes by which all executives and critical personnel report to work.
(O-25)	UNCLAS	All	Minimize the use of e-mail and web pages to confer information about operational schedules, vessel arrival and departure times, and so on. Password protect fee-for-service web pages with vessel arrival and operational information.

## 4440 (SSI) Roles, Resources, Authorities, and Responsibilities

[RESERVED]

## 4450 (SSI) Security Measures for SPOE Operations

[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-18
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

## 4500 (U) MARSEC Level 3

This section is organized as follows:

- 4510 Standard Security Procedures for MARSEC Level THREE
- 4520 Physical Security Measures
- 4530 Operational Security (OPSEC) Measures
- 4540 Roles, Resources, Authorities, and Responsibilities
- 4550 Security Measures for SPOE Operations

## 4510 (SSI) Standard Security Procedures for MARSEC Level THREE

[RESERVED]

## 4520 (SSI) Physical Security Measures

Measure	Info Security	Responsible Entity	Description
(90)	UNCLAS	All	Continue all MARSEC ONE and TWO Security Measures except measures (31), (32), (38), and (42).
(91)	UNCLAS	All vessels and facilities with required security plans, all government installations	<b>Conduct OPERATIONAL PAUSE</b> as defined in MARSEC TWO Security Measure (49). Upon receiving notification of MARSEC THREE set, conduct an operational pause while all spaces and operations ashore and afloat are reviewed. No vessels are to depart the dock or make entry into the port. Re-start operations after all-clear is confirmed by the FSO/VSO. Report the all-clear as soon as possible and no later than two hours after notification to the USCG Integrated Command Center, <b>3440.2</b> . Report suspicious activity or security breaches to 911 and the National Response Center at (800) 422-8802. For entities with approved facility or vessel security plans, begin implementing MARSEC THREE security measures after the operational pause is complete and confirm attainment of MARSEC THREE within twelve hours. Report inability (shortfalls) to attain elements of MARSEC THREE security measures immediately to the USCG Integrated Command Center. Repeat review/search procedures every 12 hours while MARSEC THREE is maintained, including report of "all clear" to the Integrated Command Center, <b>3440.2</b> .

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-19
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(92)	UNCLAS	USCG Captain of the Port	Upon MARSEC THREE set, issue a Captain of the Port order as defined in MARSEC TWO Security Measure (53) prohibiting the entry and departure of vessels except law enforcement and emergency response as part of the Operational Pause. Ban all recreational vessels on the St. Johns River from the I-295 bridge to the Ocean, on the St. Marys River and ICW from Kings Bay to the ocean, and in Port Canaveral for the duration of MARSEC THREE. Once an all-clear has been reported, grant permission for the vessel to resume operations, and lift the Captain of the Port Order only when the large majority of vessels and facilities requiring security plans have reported all-clear. Incoming vessels that cannot divert to another port must be queued and escorted to the dock, <b>3440.2</b> .
(93)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(94)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(95)	UNCLAS	ALL	Queue all commercial traffic entering or leaving the St. Johns River, St. Marys River, and Port Canaveral using the Sentinel / Gate-keeper as traffic control. Contact the Gate-keeper via VHF 21A for queuing information.
(96)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(97)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(98)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(99)	UNCLAS	All Operators	Implement MARSEC TWO Security Measures (57), (58), (59) and (60) to the maximum extent possible.
(100)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-20
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(101)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(102)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(103)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(104)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(105)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(106)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(107)	UNCLAS	All	Review security incident response plans and refresh all personnel on procedures contained therein. Place any specialized personnel and/or equipment required in stand-by status for maximum speed of response.

## 4530 (SSI) Operational Security Measures

Operational Security is defined as a systematic and analytical process by which Government agencies, commercial entities, and private citizens can deny potential adversaries information about our capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.

The information about our intentions, capabilities, or activities is known as “critical information.” Since the compromise of this critical information may allow a terrorist to gain a significant advantage, its protection involves all personnel—active, reserve, auxiliary, civilians and contractors. A concerted effort must be taken to ensure everyone is aware that the threat is real and active in all aspects of our missions.

Operational Security Measures mitigate or control vulnerabilities, threats, and usefulness of information that our adversaries may develop. These measures can include procedural changes, suppression of indicators to deny critical information, deception, preception management, intelligence countermeasures, traditional (physical) security measures, or any other action that is likely to thwart our adversary’s purposes. The Port Security Committee has recommended the following OPSEC Measures for MARSEC THREE:

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-21
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

<u>Measure</u>	<u>Info Security</u>	<u>Responsible Entity</u>	<u>Description</u>
(O-27)	UNCLAS	All	Continue all MARSEC ONE and TWO OPSEC Measures except (O-1), (O-3), (O-8), (O-9), and (O-10)
(O-28)	UNCLAS	MJTF	Within one hour of MARSEC THREE set, begin monitoring of OPSEC measures within the port and on vessels. Assure vessels, facilities, and other marine areas are using these OPSEC measures and those defined within their own security plans.
(O-29)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-30)	UNCLAS	All	To the extent possible, change the shift reporting times and operational cycles in order to maximize adversary confusion. Vary the times and routes by which all employees report to work, and consider staggered arrival times within one shift.
(O-31)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]
(O-32)	[Removed SSI Material]	[Removed SSI Material]	[Removed SSI Material]

## 4540 (SSI) Roles, Resources, And Responsibilities

[RESERVED]

## 4550 (SSI) Security Measures for SPOE Operations

[Removed SSI Material]

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-22
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

## 4600 (U) Public Access Facility

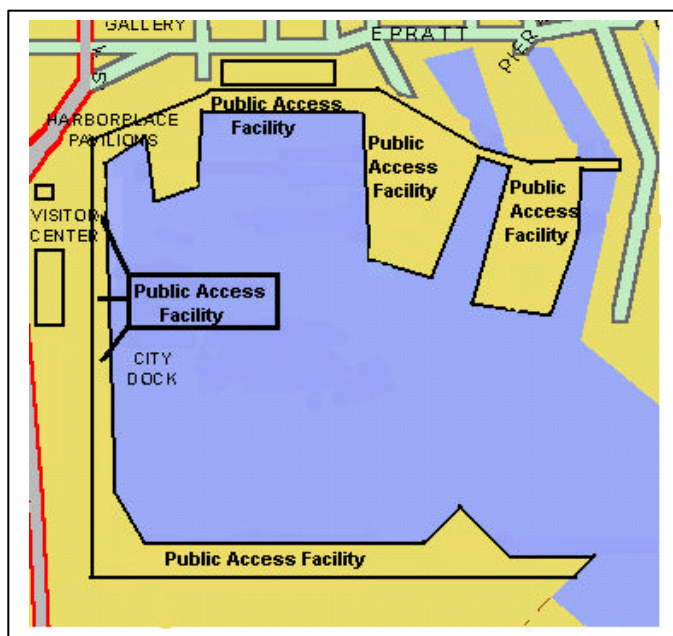
A Public Access Facility is defined as an area with public access that is primarily for recreation or entertainment purposes, and whose primary purpose is not meant to receive or service vessels regulated under 33 CFR 104. This may include a public pier, wharf, dock, waterside restaurant, or marina that contains minimal infrastructure such as only bollards, cleats, or ticket booths, or even a riverbank that contains no infrastructure.

Additionally, certain facilities subject to the security regulations in 33 CFR part 105 may petition the FMSC under the provisions of those regulations and paragraph 4610 below to be designated as Public Access Facilities in lieu of meeting the 33 CFR part 105 requirements. This section details the rules pertaining to these facilities (only). This section is organized as follows:

- 4610 Designation as a Public Access Facilities
- 4611 Designated Public Access Facilities
- 4620 Withdrawal of Designation
- 4630 Security Measures for Public Access Facilities

## 4610 (U) Designation as a Public Access Facilities

An owner or operator may send a written request to the cognizant Federal Maritime Security Coordinator requesting to be designated as a Public Access Facility in lieu of complying the requirements of 33 CFR 105. A facility designated as a Public Access Facility is not relieved from all security responsibilities. Instead, these facilities will be required to meet the measures outlined by the FMSC, and may be required to provide some additional measures of security as a condition of the FMSC designating them as a Public Access Facility.



Before granting this designation, the FMSC will consider the results of the AMS Assessment when granting an exemption. The FMSC will then notify the facility in writing that their request for designation as a Public Access Facility has been approved or disapproved. Under no circumstances may a facility regulated under 33 CFR part 105 begin operating as a Public Access Area until it has received a final designation letter from the FMSC and has implemented the minimum security measures in this plan and any additional security measures outlined in the FMSC's final designation letter. Though the facility may be exempted from the provisions of

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION:	FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-23
-----------------	----------------	-----------------	------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

33 CFR 105, the FMSC may require a written agreement (bare-bones plan) from the owner or operator of the Public Access Facility to provide adequate security at heighten MARSEC Levels as condition for granting the designation.

For example, the COTP will normally consider requiring the facility owner or operator to provide additional guards to monitor the Public Access Facility at MARSEC Levels 2 or 3 or during special events. To insure that adequate security is maintained, facility and vessel owners or operations are encouraged to cooperate with vessel owners or operators when coordinating the conditions of the COTP exemption.

In addition, this written agreement does not limit the COTP's authority to require the implementation of additional security measure to deal with specific security concerns. Figure (1) is an example of how the boundaries of a Public Access Facility could be designated. Typically, the perimeter is not bounded to allow unimpeded access to the facility.

## 4611 (U) Designated Public Access Facilities

The Federal Maritime Security Coordinator has not designated any facilities normally regulated under 33 CFR part 105 as Public Access Facilities.

## 4620 (U) Withdrawal of Designation

The COTP may withdraw the designation if the owner or operator of a Public Access Facility fails to comply with any written conditions of the designation or any additional measure ordered by the COTP. When a designation has been withdrawn from a facility that receives vessels regulated under 33 CFR part 104, the facility will be required to comply with the requirements of 33 CFR part 105. A Public Access Facility owner or operator may request in writing to be re-designated as a Public Access Facility upon rectifying unsuitable conditions.

## 4630 (SSI) Security Measures for Public Access Facilities

[Removed SSI Material]

## 4700 (U) Maritime Worker Credentials

Any personal identification credential for maritime workers accepted under the access control provisions of 33 CFR 101, Chapter 1, Subchapter H must, at least, meet the following requirements:

1. Be laminated or otherwise secure against tampering.
2. Contain the individual's full name.
3. Contain a photo which depicts the individual's current facial appearance.
4. Bear the name of the issuing authority.

The issuing authority must be a government authority, an organization authorized to act on the behalf of a government authority, or the individual's employer, union, or trade association.

VERSION DATE	V_1.0 DRAFT	CLASSIFICATION: FOUO / SSI	CONTROLLING AUTHORITY	USCG MSO JAX	ISSUING AUTHORITY	CAPT D.L. LERSCH	PAGE	4000-24
-----------------	----------------	-------------------------------	--------------------------	-----------------	----------------------	---------------------	------	---------

SENSITIVE SECURITY INFORMATION. WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.